UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,794	08/05/2003	Vincent Alan Larsen	SAGE-26,417	2708

758 7590 03/23/2007

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/635,794	LARSEN, VINCENT ALAN	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :11-10-03/10-4-04/5-31-05/7-22-05/12-27-05/3-30-06/8-18-06/11-20-06.

DETAILED ACTION

1. Claims 1-20 have been examined.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on November 10, 2003, October 4, 2004, May 31, 2005, July 22, 2005, December 27, 2005, March 30, 2006, August 18, 2006, and November 20, 2006, are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

3. Claims 1-11 are objected to because of the following informalities: claim 1, line 14, is missing the word "the" after "operating on" and before "password"; claim 8 cites the word "number" twice in a row. The remaining claims, 2-11, are dependent upon claim 1 and therefore inherit its deficiencies. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 1 recites the limitation "calculating a first key" in lines 12 and 14. The presence of two "first keys" that are operated on by a server and a client is unclear as to which key is the first key.

7. Claims 2-11 are dependent upon claim 1 and therefore inherit its deficiencies.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mauro et al. (U.S. Patent Pub. No. 2002/0146128) in view of Euchner (U.S. Patent No. 7,007,164).

Regarding claims 1 and 12, Mauro et al. teaches a method/system of performing a key exchange between a client and a server having a process-based security system comprising the steps of:

- Sending user identification information from the client to the server (paragraph 0031, key exchange includes identification);

- Modifying the task structure of the client by the server to reflect a pending request for key exchange (paragraph 0036, a semaphore is set to lock other processes from accessing a shared resource);
- Generating a first random number; sending the first random number to the client; calculating a first key using a transformative function operating on the first random number by the server; calculating a first key using the transformative function operating on the first random number by the client; using the result of the calculated first key as a first key (paragraph 0037, a Diffie-Hellman key exchange takes place by generating random numbers by the client and the server and generating a common key by using the random number); and
- Modifying the task structure of the client by the server to reflect the completion of the key exchange (paragraph 0036, the semaphore is cleared to allow other processes to access the shared resource).

Mauro et al. does not teach retrieving a password associated with the user identification information by the server; entering a password at the client; calculating a first key using a transformative function operating on the password by the server; and calculating a first key using the transformative function operating on the password by the client.

Euchner teaches retrieving a password associated with the user identification information by the server; entering a password at the client; calculating a first key using

a transformative function operating on the password by the server; and calculating a first key using the transformative function operating on the password by the client (fig. 1 and col. 3, line 58 through col. 4, line 19).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine retrieving a password and calculating a key based on the password, as taught by Euchner, with the method/system of Mauro et al. It would have been obvious for such modifications because using a password as part of a Diffie-Hellman key exchange between a client and a server enables the client and server to already have the "secret" prior to the key exchange. The password provided by the client for key exchange is already stored on the server.

Regarding claim 2, Mauro et al. as modified by Euchner teaches wherein said client is a process executed on the server (see figure 1 of Mauro et al.).

Regarding claim 3, Mauro et al. as modified by Euchner teaches wherein said client is a process running on a remote machine (see fig. 1, ref. num 14 of Mauro et al., a DSP is a processor that can run on any machine, local or remote, that has a processor).

Regarding claims 4 and 15, Mauro et al. as modified by Euchner teaches wherein said transformative function is a hash function (see fig. 1 and col. 3, line 58 through col. 4, line 19 of Euchner).

Regarding claims 5 and 16, Mauro et al. as modified by Euchner teaches wherein said transformative function is a keyed MD5 signature function (see paragraph 0028 of Mauro et al.).

Regarding claims 6 and 17, Mauro et al. as modified by Euchner teaches wherein the first key is used for communication using symmetric encryption (see col. 3, lines 20-22 of Euchner).

Regarding claims 7 and 20, Mauro et al. as modified by Euchner teaches wherein said first random number is generated using noise (see paragraph 0037 of Mauro et al., a Diffie-Hellman key exchange can use any source for a random number, such as noise).

Regarding claim 8, the examiner takes Official Notice that said first random number is sixteen bits in length. The combination of references teaches using a random number between the client and the server in order to use a Diffie-Hellman key exchange. Diffie-Hellman does not require a certain key length, so a 16 bit key length

would suffice depending on the application. A longer key length would provide more security.

Regarding claims 9 and 18, Mauro et al. as modified by Euchner teaches further comprising the steps of:

- Generating a second random number by the server; sending the second random number to the client; calculating a second key using the transformative function operating on the password and second random number by the server; calculating a second key using the transformative function operating on the password and second random number by the client; using the calculated second key as a second key (see fig. 1 of Euchner, the client and server each create a key used for communication with each other).

Regarding claims 10 and 19, Mauro et al. as modified by Euchner teaches wherein said first key is used to encrypt communications from the client to the server and said second key is used to encrypt communications from the server to the client (see fig. 1, ref. num 106 and 108 of Euchner).

Regarding claims 11 and 14, Mauro et al. as modified by Euchner teaches where said retrieved password is cleartext (see col. 4, lines 14-15 of Euchner, Diffie-Hellman key exchange allows all values to be sent in the clear, except for the keys, i.e., g^a or g^b).

Regarding claim 13, Mauro et al. as modified by Euchner teaches wherein the key exchange server processor is communicably connected to the client by a network (see col. 4, lines 61-67 of Euchner).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/19/07